REMARKS

Claims 24-26 are canceled and claims 33-36 were previously canceled. Thus, claims 1-23, 27-32 and 37-50 are now pending.

I. ISSUES RELATING TO PRIOR ART

A. CLAIMS 1-3, 5, 7, 11, 14-16, 18-20, 24, 27-29, 31, 32, 37-39, 41-43, 47

Claims 1-3, 5, 7, 11, 14-16, 18-20, 24, 27-29, 31, 32, 37-39, 41-43, and 47 stand rejected under 35 U.S.C. 103 as allegedly unpatentable over Buer et al. in view of Markham. The rejection is respectfully traversed.

Each of the independent claims features receiving and storing, **during initial establishment of a secure control channel,** an identifier associated with the quality of service; examining an encrypted packet; **without decrypting the encrypted packet,** determining whether the identifier associated with the quality of service is present **in a profile portion of the encrypted packet**; and in response to determining that the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet.

In one embodiment, a network element could receive and store, as part of establishing an IKE security association, an IKE identifier or other unique identifier, then receive an encrypted packet and without decrypting the packet, determine whether the encrypted packet contains (in the profile portion of the packet) the identifier that is associated with a particular quality of service treatment, and then apply the particular QoS treatment to the packet.

Therefore, QoS can be applied to encrypted packets in which QoS markings are normally impossible to read because of the encryption. The identifier signaling a particular QoS treatment is carried in a profile portion of the encrypted packet, which is normally used for security profile information and not QoS information. The identifier is received and stored during initial establishment of a secure control channel, for example, when an IPSec security association is negotiated.

The Office Action relies on paragraphs 76-77 of Buer, which state:

> [0076] When an encrypted packet is received by the network controller/packet processor **220**, the network controller/packet processor **220** reads the identifier in the packet to determine which security association should be used with that packet (block **614**). For example, if the identifier consists of the address of the security association the network controller/packet processor **220** reads the data from that address in the database **240**. Alternatively, if the security association includes the identifier, the network controller/packet processor **220** may scan the database for a security association that contains an identifier that matches the identifier for the packet. The network controller/packet processor **220** sends the packet and the security association to the cryptographic accelerator **236** (block **616**).
>
> [0077] The cryptographic accelerator **236** decrypts the security association using the key stream and sends the decrypted session key to the cipher engine **424A**, **424B** (block **618**). The cipher engine **424A**, **424B** decrypts the encrypted packet using the session key (block **620**) and sends the decrypted packet back to the network controller/packet processor **220**. The network controller/packet processor **220**, in turn, sends the packet to the host processor **224** for processing (block **622**).

Buer reads an identifier in a packet merely to determine what security association is involved—**not to determine what QoS to apply**. Any "service" described in Buer merely involves conventional decryption based on a particular security association. Buer has no description of **applying a quality of service treatment** to an encrypted packet based on an identifier in the encrypted packet. The identifier is only used to determine what SA corresponds to the packet, not what quality of service to apply, because the packet is encrypted and Buer cannot determine how to apply QoS for an encrypted packet because payload values can't be read.

While Buer can extract an SA identifier without decryption, the identifier is usable only to determine the SA, and Buer requires decrypting the packet to determine what QoS to apply. The claimed approach does not require decryption—it relies on a QoS identifier value carried in a profile portion, such as an ISAKMP profile in a form of header of the packet. Because the claimed approach can use an identifier in the profile portion, the claimed approach can determine what QoS to apply **without decryption,** as expressly claimed.

Markham does not cure the deficiencies of Buer. The Office Action relies on paragraphs 16, 60, and 89 of Markham, and Table 1. Paragraph 16 generically refers to QoS without suggesting applicants' specific approach. Paragraph 60 states that Markham can provide QoS in the form of bandwidth management by prioritizing traffic sent from the host, but does not explain how that would be accomplished. Most likely, Markham would prioritize all traffic on the basis of a host source IP address so that one host could not hog too much bandwidth. Such an implementation would not involve the first step of applicants' method in which a QoS identifier is received when a secure control channel is set up, or examining a profile portion of the encrypted packet, as claimed.

Markham paragraphs 88-92 propose three forms of QoS control that do not involve determining whether a QoS identifier is in a profile portion of the encrypted packet, as claimed—instead, Markham suggests (1) using an 802.1p priority tag value in a special field of the IP header, (2) using a priority filter on the network interface card that is triggered by traffic level, or (3) examining a ToS bit in the IP header, if present. All three approaches involve technical implementations that are completely different from applicants' approach. Approach (1) requires both endpoints to be compatible with 802.1p and to use the defined header field each time that packets are sent; instead, applicants' approach uses the initial establishment of a secure control channel to set up the QoS identifier and uses the profile portion. Approach (2) can only accomplish bandwidth management and cannot apply different QoS to different packets coming from the same host; it does not involve carrying a QoS identifier in the packet. Approach (3) is workable only for reading the ToS bit in the outer header of a packet in which the payload encapsulates an encrypted original packet. Thus, approach (3) assumes that a sender sets QoS as part of IPSec encryption and encapsulation, in the outer header of the packet, but this is not a conventional operation in IPSec—normally, the relevant ToS bit is only available in the *inner* packet, which is encrypted and therefore unreadable. In any case, the ToS bit is not carried in the profile portion, as claimed, and does not involve receiving an identifier during initial

establishment of a secure control channel, as claimed. For all these reasons, Markham **teaches away** from the claimed approach and has no suggestion to use initial establishment of a secure control channel, and the profile portion of the packet, for QoS control.

Further, Buer does not perform the first setup step in which a QoS identifier is received during initial establishment or negotiation of a secure control channel.

Still further, Buer does not obtain the identifier from a profile portion of the encrypted packet, as claimed.

Markham does not cure the deficiencies of Buer identified above. Markham has no teaching that relates in any way to the differences identified above with respect to Buer.

For at least these reasons, a combination of Buer and Markham fails to provide the subject matter of the independent claims. All independent claims (1, 11, 27, 37) recite steps or apparatus elements that provide for the distinguishing features identified above. Thus, all independent claims and all claims that depend directly or indirectly from them include the features of claim 1 that distinguish Buer and Markham.

For at least the foregoing reasons, the rejection of claims 1-3, 5, 7, 11, 14-16, 18-20, 24, 27-29, 31, 32, 37-39, 41-43, and 47 is traversed. Reconsideration is respectfully requested.

B. CLAIMS 4, 8, 17, 21, 30, 40, 44—BUER AND MARKHAM IN VIEW OF PIPER

Paragraphs 9-10 of the Office Action reject claims 4, 8, 17, 21, 30, 40, and 44 under 35 U.S.C. 103(a) as allegedly unpatentable over Buer and Markham in view of Piper. The rejection is respectfully traversed.

The Office Action relies on Piper pp. 19-20 to show that the IKE ID comprises the identifiers recited in claim 4 and similar claims, and the use of ISAKMP in claim 8 and similar claims. However, Piper has no description or suggestion of receiving and storing, **during initial establishment of a secure control channel,** an identifier associated with the quality of service; examining an encrypted packet; **without decrypting the encrypted packet,** determining

whether the identifier associated with the quality of service is present **in a profile portion of the encrypted packet**; and in response to determining that the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet, as recited in claim 1 and all other independent claims.

Thus, Piper does not cure the deficiency of Buer with respect to the preceding features, and therefore any combination of Piper with Buer cannot provide the complete invention as recited in claim 4 or similar claims, or as recited in claim 8 and similar claims. Reconsideration is respectfully requested.

C. CLAIMS 9, 10, 12, 22, 23, 25, 35, 36, 45, 46, 49-50—BUER IN VIEW OF VALENCI

Paragraph 12 of the Office Action rejects claims 9, 10, 12, 22, 23, 25, 35, 36, 45, 46, and 49-50 under 35 U.S.C. 103(a) as allegedly unpatentable over Buer and Markham in view of Valenci. The rejection is respectfully traversed.

The Office Action relies on Valenci to show pre-classification of packets. However, Valenci has no description or suggestion of receiving and storing, **during initial establishment of a secure control channel,** an identifier associated with the quality of service; examining an encrypted packet; **without decrypting the encrypted packet,** determining whether the identifier associated with the quality of service is present **in a profile portion of the encrypted packet**; and in response to determining that the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet, as recited in claim 1. Since Valenci does not cure the deficiency of Buer and Markham with respect to the preceding features, and therefore any combination of Valenci with Buer and Markham cannot provide the complete invention as recited in claim 9 or other similar claims.

Regarding claim 10, the Office Action relies on Valenci paragraphs 27, 34, 35, but the only "service" alluded to in Valenci is conventional encryption or "cryptographic processing." These paragraphs of Valenci say nothing about **applying QoS treatment to a packet based on**

both an identifier found in the encrypted packet and its pre-classification, as recited in claim 10 when read in combination with claim 1, or other claims similar to claim 10.

Reconsideration is respectfully requested.

E. CLAIMS 13, 26—BUER IN VIEW OF YLONEN

Paragraph 13 of the Office Action rejects claims 13 and 26 under 35 U.S.C. 103(a) as allegedly unpatentable over Buer and Markahm in view of Ylonen. The rejection is respectfully traversed.

The Office Action relies on Ylonen to show copying at least one bit into a header to identify a characteristic of the packet. However, Ylonen has no description or suggestion of receiving and storing, **during initial establishment of a secure control channel,** an identifier associated with the quality of service; examining an encrypted packet; **without decrypting the encrypted packet,** determining whether the identifier associated with the quality of service is present **in a profile portion of the encrypted packet**; and in response to determining that the identifier is present in the encrypted packet, applying the associated quality of service to the encrypted packet, as recited in claim 1. Since Ylonen does not cure the deficiency of Buer with respect to the preceding features, and therefore any combination of Ylonen with Buer cannot provide the complete invention as recited in claim 13 and 26. Reconsideration is respectfully requested.

II. CLAIMS 14-26

Claims 14-26 are revised merely for the purpose of clarity to use a more conventional form of "computer-readable medium" claim. No substantive change is introduced.

III. CONCLUSIONS

Based on the foregoing, all the present claims are in condition for allowance.

Applicants hereby petition for an extension of time under 37 C.F.R. 1.136 for one (1) month and any other time period necessary to make this paper timely filed. The petition fee is submitted concurrently herewith.

No fee is believed to be due for this paper. However, if any applicable fee is missing or insufficient, the Director is hereby authorized to charge any applicable fee to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

/ChristopherJPalermo#42056/
Christopher J. Palermo
Reg. No. 42,056

Dated: November 9, 2007

2055 Gateway Place Suite 550
San Jose, California 95110
Tel: (408) 414-1080x202
Fax: (408) 414-1076